

Telecom Carrier توفر حل الأمان السحابي الأول من نوعه



ينتشارك BT مع شركة Cisco و SecureLogix لمساعدة العملاء على تحديد تهديدات الصوت والبيانات من خلال حل متكامل واحد.

التحدي

إن BT هي الشركة الرائدة في مجال الاتصالات العالمية مع العملاء في أكثر من ١٧٠ دولة، تقدم خدمات الخط الثابت واتصال واسع النطاق ومنتجات وخدمات الهاتف المحمول والتلفزيون إلى العملاء وشركات العمل المؤسسين والقطاع العام. تعتبر خدمات BT العالمية هي واحدة من خطوط الشركة الأربع التي تتعامل مع العميل، مما يوفر خدمات تكنولوجيا المعلومات المتصلة بالشبكة المدارة لعملاء الشركة الكبيرة والقطاع العام.

مع زيادة ظاهرة "اختراق الأنظمة الإلكترونية"، التي تعمل على الاختراق لأغراض ذات دوافع سياسية، أصبح أمان الإنترنت من أهم الأولويات لكثير من عملاء BT. على حد قول "جيف شميث"، الرئيس العالمي، لاستمرارية العمل والأمان والقواعد الحاكمة لخدمات BT العالمية أن "يعاني أيضًا ٩٨ بالمائة من الشركات التي تضررت بسبب المخترقين من الاتصال عن طريق الاحتيال. ويستخدم العديد من المخترقين هذا الاحتيال لتمويل أنشطتهم." في الواقع، تُقدر خسائر الاحتيال الخاصة بالاتصالات عن بعد بحوالي ٤٠ مليار دولار أمريكي سنويًا^١.

لمعالجة هذه المشكلة، بدأ BT في تطوير محرك تحليل البيانات المرئية الذكية الذي يمكن ان يقوم بتحسين الوعي الموقفي وتحديد التهديدات الصوتية والبيانات في الوقت الفعلي. يسحب الحل جميع المعلومات من الشبكة، ويقوم بتعيين خط أساسي، وبعد ذلك تحديد مكان الأشياء غير الطبيعية الموجودة ضمن بنية الشبكة. بواسطة التعيين المرئي لهذه الحالات غير الطبيعية، يتمكن BT من تحديد وتقليل التهديدات بسرعة أكبر وبسهولة مقابل مراجعة مجموعة كبيرة من البيانات.

بدأ فريق "شميث" في بناء محرك التحليلات للاستخدام داخليًا وخارجيًا لعملاء المؤسسات. كان الهدف هو تعزيز وجود خدمة مراقبة التهديد للأمن من BT، حيث في ذلك الوقت تم التركيز على خدمات أمان البيانات بشكل أساسي. ومع ذلك، عرف الفريق أن هذه المهمة تحتاج إلى تقنيات رائدة في السوق الخاصة بالأمان والبيانات ومجال الصوت. وهذا هو سبب تحول الشركة إلى شركاء Cisco و SecureLogix.

الملخص التنفيذي

- اسم العميل: BT
- الصناعة: الاتصالات السلكية واللاسلكية
- الموقع: لندن، المملكة المتحدة
- عدد الموظفين: ٩٢٦٠٠

التحدي

- تحسين الأمان لشبكات الصوت في المؤسسة
- لا يوجد عرض شامل لبيئة الشبكة
- تحسين أمان البيانات بواسطة تأمين شبكة الصوت

الحل

- تعبئة الخدمة السحابية BT Assure
- Analytics هي أداة مرئية تساعد على تحديد وتقليل الصوت وتهديدات البيانات
- يوفر الجيل الثاني من موجهات الخدمات المتكاملة من شركة Cisco خدمات الصوت والبيانات على نظام أساسي واحد وتسمح واجهة برمجة التطبيقات (API) الخاصة بخدمات بوابة UC من Cisco للشركاء بإنشاء تطبيقات الأمان لحركة مرور الصوت، سواء عن طريق أنظمة الاتصال TDM أو SIP.
- نهج الصوت SecureLogix وتطبيق الأمان



الحل

من خلال تكامل نهج الصوت وتطبيقات الأمان مع بوابات الصوت من Cisco، يعتبر SecureLogix هو أول شريك لتطور التكنولوجيا من Cisco للاستفادة من واجهة برمجة التطبيقات (API) الخاصة بخدمات بوابة Cisco® UC. إن واجهة API الخاصة بخدمات بوابة UC من Cisco هي واجهة برمجة التطبيق (API) المستند إلى الويب الذي يتم دعمه على الجيل الثاني من أجهزة توجيه خدمات Cisco المتكاملة (ISR G2) مع Cisco Unified Border Element (CUBE) لخط الاتصال SIP وبوابة TDM من Cisco لخطوط اتصال الإرسال المتعدد للتقسيم الزمني (TDM).

باستخدام SecureLogix و Cisco، يحتوي BT الآن على الوصول الكامل للبيانات والصوت، سواء كان يعتمد على SIP أو TDM لكي يتم توفير خدمات الأمان السحابية المتكاملة على نظام أساسي واحد، Cisco ISR G2.

قال "جو اودونيل" نائب رئيس في قسم تطوير الأعمال في SecureLogix، أن "واجهة برمجة التطبيقات (API) الخاصة بخدمات بوابة UC من Cisco تمنحنا بيانات غنية في الوقت الفعلي التي تكون تاريخياً قد تحتاج من العملاء لنشر أجهزة الأمان المخصصة. عند الاستخدام بالاقتران مع Cisco ISR G2، تسمح واجهة API بنشر وحل مشاكل العملاء لدينا بشكل أسرع، بغض النظر عن المكان الذي يقع فيه." وتتمكن شركة Cisco و SecureLogix معاً من تقديم حل كامل يساعد موفري الخدمة والمؤسسات على تحقيق مستوى جديد من إمكانية الرؤية والتحكم بشبكة الصوت.

يقول شميت أن "بفضل Cisco و SecureLogix، يمكن أن يوفر BT الآن حل الأمان الأول على نطاق المؤسسة الخاص بالصناعة لكل من البيانات والصوت، مما يشمل أنظمة اتصال TDM و SIP، المتكاملة على نظام أساسي واحد، Cisco ISR G2. "ويمكننا شرح وتقديم الحل الذي تم تعيينه واللازم للعمل اعتماداً على المتطلبات الأكثر ملاءمة لعملائهم، وليس ما يتناسب مع البائع أو الناقل." ولذلك، لا يتعين على عملائهم إجراء تغييرات كبيرة بالبنية لنشر الحل، ويمكنهم استخدام أي ناقل لخدمات النقل المتطورة، حتى إذا كانت ليس من BT.

يضيف شميت: "أن الأهم من ذلك هو حقيقة أن BT يمكنه الآن تحديد ما هو معروف بالهجمات "المنخفضة والبطيئة" المدمرة بشكل خاص". كما صرح شميت أن "هذه هي الهجمات التي تحدث خلال فترة زمنية طويلة، لذلك لا تظهر بالفعل على الرادار الخاص بأي شخص". "ولكن ما يسمح به حل Cisco و SecureLogix هو النظر إلى هذه الأشياء غير الطبيعية والمختلفة. وبعد ذلك يرتبط سير العمل بأنظمة التذاكر التي تعمل على تنبيه العميل من أن هناك شيئاً يستحق النظر إليه ومعالجته."

إن خدمة BT Assure Analytics التي تقوم الآن بتحديد التهديدات للصوت والبيانات بشكل عام، تعتمد أيضاً بشكل كبير على Cisco UCS® Express، وهي شفرة الخادم التي تعمل على Cisco ISR G2. يقول "اودونيل" أن "بواسطة نظام Cisco UCS Express الموجود على Cisco ISR G2، نحن نتمكن بسهولة من تقديم حساب مقارب ونظام أساسي للشبكات الذي يقوم باستضافة خدمات البنية الهامة SecureLogix و BT". "كما يسمح لـ BT بتوسيع نطاق البنية السحابية، بينما يتم زيادة الكفاءات في البيئة جميعها على نظام أساسي واحد."

المخلص التنفيذي (مستمر)

النتائج

- اكتساب ميزة تنافسية كموفر أول لتقديم الصوت الفردي واللوحه المرئية لتأمين البيانات بعملاء المؤسسة بشكل عام.
- تقديم التطبيق السحابي الذي يمكنه العمل بخدمات النقل SIP أو TDM الخاص بأي موفر خدمة.
- تمكين العملاء في المؤسسة للحصول على إمكانية الرؤية الواضحة والتحكم بشبكة الصوت وحل مشاكل الأمان في وقت أسرع من أسابيع إلى دقائق

"يمكننا الآن أن نقدم لعملائنا الأمان الصوتي على نطاق المؤسسة، بغض النظر عن موفر الخدمة وسواء كان يستخدمون أنظمة الاتصال TDM أو SIP. يمكن أن نقدم لهم الحد الأقصى للرؤية الواضحة والتحكم بوحدة من أكبر الأصول الموجودة لديهم في الشركة."

— جيف شميت

الرئيس العالمي، لاستمرارية العمل والأمان والقواعد الحاكمة خدمات BT العالمية

النتائج

تأمين أكثر من مجرد مؤسسة

يتم استخدام BT Assure Analytics ليس فقط من قبل المؤسسات على الصعيد العالمي، ولكن يتم أيضًا استخدام محرك الأمان من قبل BT نفسه. تم تطوير الأداة في الأصل كوسيلة لـ BT للحد من سرقة الكابلات النحاسية. قام BT بالاستفادة من محرك التحليلات للبحث عن أنماط السرقة في اتجاهات متعددة. يستنتج "شملت" قائلًا: "إننا قمنا بتحديد الفرصة لاستخدام البيانات لتشغيل أسلوب أكثر فاعلية لمعالجة مشكلة سرقة الكابل، حيث يبدأ في الترجمة إلى توفير التكاليف المباشرة". بالإضافة إلى ذلك، أفضل سمعة للعلامة التجارية بواسطة منع مدة التوقف للعمل نظرًا لسرقة الكابلات. أما الآن فقد تم توسيع الأداة إلى تطبيقات الأمان الأخرى والخدمات لمساعدة المؤسسات بشكل عام على محاربة احتيال وسرقة الصوت والبيانات.

الخطوات التالية

نظرًا لأن موثر الخدمة الأول والوحيد يقدم طريقة عرض أمان صوت وبيانات واحد، لدى BT الآن ميزة تنافسية مختلفة في سوق الاتصالات عن بعد. يقول شملت أن "يمكننا الآن أن نقدم لعملائنا أمان الصوت على نطاق المؤسسة بالإضافة إلى أمان البيانات، بغض النظر عن موثر الخدمة وسواء كانوا يستخدمون نظام اتصال TDM أو SIP، ويضيف: "يمكن أن نقدم لهم الحد الأقصى للرؤية الواضحة والتحكم بوحدة من أكبر الأصول الموجودة لديهم في الشركة."

بواسطة Cisco وتقنية SecureLogix، شهد بالفعل BT وعلاؤه باستخدام محرك BT Assure Analytics تحسين في أوقات حل المشاكل. كما أعلن شملت أن "مشاكل الصوت التي قد تستغرق أسابيع أو حتى أشهر لمعالجتها يمكن أن يتم حلها في دقائق معدودة".

على الرغم من مجموعة فوائد العمل التي لا حصر لها التي تأتي مع تقديم أمان جديد، ويعتبر التأثير الفعلي لهذا المشروع هو حول إحباط هجمات الشبكة ككل. وأضاف شملت أن "ذلك يعتبر مشكلة عالمية بالفعل". "إنه فعال. ومدمر. ونحن نعتقد بشكل إجمالي أن BT و Cisco و SecureLogix هم أقوى الشركات لمساعدة العملاء في المؤسسات لدينا لمحاربة هذه الظاهرة. وهدفنا ليس فقط توحيد البيانات ولكن أيضًا تأمين الصوت كممارسة أفضل لتكنولوجيا المعلومات."

بالنظر إلى المستقبل، ستستمر خدمات BT العالمية مع تطور خدمة BT Assure Analytics للحصول على وضوح أكثر بالصوت وبيانات البيانات. ويضيف شملت أن "كلما زادت المعلومات التي نحصل عليها، كان ما نحصل عليه هو الأفضل"، "لذلك من المهم أن نستمر في العمل بشكل وثيق للغاية مع شركائنا، Cisco و SecureLogix، للمساعدة على ضمان أن نحصل على الأنواع الصحيحة من التنبيهات والمعلومات من مكونات المتعددة لبنية Cisco."

الحصول على مزيد من المعلومات

لمعرفة المزيد حول واجهة برمجة التطبيقات (API) الخاصة بخدمات بوابة UC من Cisco، يُرجى زيارة: <http://developer.cisco.com/web/gsap>
لمعرفة المزيد حول Cisco Unified Border Element (CUBE)، يُرجى زيارة: www.cisco.com/go/cube
لمعرفة المزيد حول الشبكة الذكية السحابية من Cisco، يُرجى زيارة: www.cisco.com/en/US/netsol/ns1172/networking_solutions_solution_category.html
لمعرفة المزيد حول Cisco ISR G2، يُرجى زيارة: www.cisco.com/go/isr
لمعرفة المزيد حول Cisco UCS G2، يُرجى زيارة: www.cisco.com/go/ucse
لمعرفة المزيد حول حل Cisco Cloud Connected، يُرجى زيارة: www.cisco.com/go/cloudconnected
لمعرفة المزيد حول SecureLogix، يُرجى زيارة: www.SecureLogix.com
لمعرفة المزيد حول BT، يُرجى زيارة: www.bt.com

قائمة المنتجات

- Cisco UC Gateway Services API •
- Cisco Unified Border Element • ((CUBE
- عبارات TDM من Cisco •
- Cisco UCS Express •
- الجيل الثاني من أجهزة توجيه خدمات Cisco المتكاملة (ISR G2) •
- BT Assure Analytics •
- نهج الصوت SecureLogix وتطبيق الأمان •



إن Cisco تقدم هذه النشرة كما هي دون ضمان من أي نوع، سواء صريحاً أم ضمنياً، بما في ذلك الضمانات الضمنية الخاصة بتجارية المنتج أو ملائمة لأي غرض معين. بعض التشريعات في بعض البلدان لا تسمح بإخلاء مسؤولية عن أي ضمانات صريحة أو ضمنية وبالتالي فإن هذا البيان بالإفكار قد لا يسري عليك.

المقر الرئيسي في أوروبا
Cisco Systems International BV Amsterdam
هولندا

المقر الرئيسي لدول آسيا والمحيط الهادئ
Cisco Systems (USA) Pte, Ltd.
سنغافورة

المقر الرئيسي بأمريكا
Cisco Systems, Inc.
سان هوزيه، كاليفورنيا

يوجد لدى Cisco أكثر من ٢٠٠ مكتب في جميع أنحاء العالم. تتوفر قائمة بالعناوين وأرقام الهاتف وأرقام الفاكسات على موقع شركة Cisco على الويب التالي www.cisco.com/go/offices.

حقوق النشر © محفوظة لعام ٢٠١٢ لشركة Cisco و/أو الشركات التابعة لها. جميع الحقوق محفوظة. تعد Cisco و Cisco علامتين تجاريتين أو علامتين تجاريتين مسجلتين لشركة Cisco و/أو الشركات التابعة لها في الولايات المتحدة والبلدان الأخرى. "لعرض قائمة بالعلامات التجارية الخاصة بشركة Cisco، انتقل إلى عنوان URL هذا: www.cisco.com/go/trademarks. العلامات التجارية الخاصة بالجهات الخارجية الواردة في هذا المستند هي ملكية خاصة بأصحابها. كما أن استخدام كلمة "الشريك" لا يشير ضمناً إلى وجود علاقة شراكة بين شركة Cisco وأي شركة أخرى. (1110R)